



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,876	04/04/2005	Marc Joye	1032326-000285	4960

21839 7590 04/30/2009
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2431

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

04/30/2009

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No. 10/509,876	Applicant(s) JOYE ET AL.	
	Examiner Christopher A. Revak	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 December 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-24 is/are rejected.
- 7) ☒ Claim(s) 7-20 and 23 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 2-24 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 2-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 2-24 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The claimed method including steps of selection of blocks of instructions which is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. The examiner notes that the preamble of claim 21 recites of a "method for implementing

Art Unit: 2431

cryptographic calculation in an electronic device" which is intended use since no positive steps of the device is recited in the body of the claim.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher et al, U.S. Patent 6,278,783.

As per claim 2, it is taught wherein the predefined number is variable from one predefined block of instructions to another (col. 6, lines 28-63).

As per claim 3, it is disclosed wherein the common set of instructions comprises at least one calculation instruction that is equivalent to a calculation instruction of each predefined block in the context of a covert channel attack (col. 2, lines 10-24).

As per claim 4, it is taught wherein the common set of instructions also comprises an instruction to update a loop pointer indicating a number of executions already performed with the common set of instructions (col. 13, lines 9-41).

As per claim 5, it is disclosed wherein the common set of instructions also comprises an instruction to update a state pointer indicating whether the predefined number has been reached (col. 13, lines 9-41).

As per claim 6, it is taught wherein the value of the loop pointer is a function of the value of the input variable and/or number of instructions in the selected block of instructions (col. 13, lines 9-41).

As per claim 21, it is taught of a method for implementing a cryptographic calculation in an electronic device, comprising the following steps selecting a block of instructions from amongst a plurality of predefined blocks of instructions, as a function of an input variable; and executing a set of instructions that is common to the plurality of predefined blocks of instructions a predefined number of times, wherein said predefined number is associated with the selected block of instructions (col. 1, line 66 through col. 2, line 43; col. 6, lines 28-63).

As per claim 22, it is disclosed of wherein the value of the state pointer is a function of the value of the input variable and/or of the number of instructions in the selected block of instructions (col. 13, lines 9-41).

As per claim 23, it is taught wherein said several inputs comprise a matrix (col. 2, line 43 through col. 3, line 9).

As per claim 24, it is disclosed wherein said electronic device is a chip card (col. 14, lines 1-8).

Allowable Subject Matter

6. Claims 7-20 and 23 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 517-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2431